WEST Search History

DATE: Saturday, May 03, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L20	L2 and hasebe	0	L20
	DB=PGPB,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L19	L17 and (document with protect$)	2	L19
L18	L17 and (document with protect$) and authori$	1	L18
L17	L16	29	L17
	DB=PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L16	(embed$ adj (data or document)) and ole	29	L16
	DB=JPAB,EPAB,DWPI; THES=ASSIGNEE; PLUR=YES; OP=OR		
L15	L14 and l13	0	L15
L14	L12 and authori$	6	L14
L13	L12 and (document with protect$)	2	L13
L12	(embed$ adj (data or document))	489	L12
L11	(embed$ adj (data or document)) and ole	0	L11
L10	(compound$ same document same protect$)	14	L10
L9	(compound$ same document same protect$) and ole	0	L9
L8	ole and (compound$ with document with protect$)	0	L8
L7	ole and (compound adj document)	0	L7
	DB=USPT,JPAB,EPAB,DWPI; THES=ASSIGNEE; PLUR=YES; OP=OR		
L6	(takayuki near2 hasebe) and (compound adj document)	0	L6
	DB=JPAB,EPAB,DWPI; THES=ASSIGNEE; PLUR=YES; OP=OR		
L5	(takayuki near2 hasebe) and (compound adj document) and ole	0	L5
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L4	l2 and (compound$ adj document).clm.	0	L4
L3	l2 and ((compound$ adj document) and (data with protection)).clm.	0	L3
L2	(compound$ adj document) and ole and (data with protection)	15	L2
L1	((707/514 |707/515 |707/516)!.CCLS.)	0	L1

reviewed

reviewed

END OF SEARCH HISTORY

L13: Entry 1 of 2 File: DWPI Oct 26, 2000

DERWENT-ACC-NO: 2001-040814
DERWENT-WEEK: 200111

TITLE: Protection system of electronic document e.g. letter, enables or disables selected operations on file operating system or application program, based on communication from protection component at destination side

INVENTOR: MUTHUSWAMY, S; RAMAMURTHY, A

PATENT-ASSIGNEE: MOTOROLA INC (MOTI)

PRIORITY-DATA: 1999US-0292207 (April 15, 1999)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 200064095 A1	October 26, 2000	E	018	H04L009/00
AU 200043396 A	November 2, 2000		000	H04L009/00

DESIGNATED-STATES: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 200064095A1	April 11, 2000	2000WO-US09645	
AU 200043396A	April 11, 2000	2000AU-0043396	
AU 200043396A		WO 200064095	Based on

INT-CL (IPC): H04 L 9/00

ABSTRACTED-PUB-NO: WO 200064095A

BASIC-ABSTRACT:

NOVELTY - A protection component (150) at the side of destination (110), reads the encrypted protection flag (130) embedded within the file (120) stored in source (100) and communicates it to operating system (160) and application program (170). The selected operations on readout file by the system or program are enabled or disabled, based on the communication from the protection component at the destination side.

DETAILED DESCRIPTION - The protection component (140) of source sets the protection flag to define a level of protection for the file, and transmits it to the protection component (150) at the destination side, on demand through a communication link (180). The operations that are to be performed with the file read out from the source, are selected from a group consisting of the file access, file operations, file manipulation, transmission, insertion, clipboard and printing. The source consists of a file, protection flag associated with the file and the protection component that set flag to define a level of protection for the file. An INDEPENDENT CLAIM is also included for electronic document content unauthorized reusage preventing system.

USE - In e.g. internet, local area network (LAN) for protecting electronic documents including letters, specifications, control drawings, spread sheets, artwork, blue prints, video images output from scanners and routine business forms used for business and non-business applications in homes, offices.

ADVANTAGE - Controls security of file by enabling or disabling the selected operational functionalities of the operating system and/or the application program at the destination side based on the communication from protection component, reliably. When the computer user accesses the protected file through the application program, the view of the file exhibiting all the enforced protection levels is provided to the user, thus preventing the user from generating duplicate copies of the entire or a portion of original content. The security information is embedded in the document by the flag in specific format, so that the flag is read by the operating system or application program to invoke specific restrictions on the operation that is performed on that document.

DESCRIPTION OF DRAWING(S) - The figure shows schematic chart depicting electronic document protection system.

Source 100

Destination 110

File 120

Encrypted protection flag 130

Protection components 140,150

Operating system 160

Application program 170

ABSTRACTED-PUB-NO: WO 200064095A
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/3

DERWENT-CLASS: T01 W01
EPI-CODES: T01-D01; T01-H07C1; T01-H07C3C; T01-H07C5E; T01-J12C; W01-A05;

DERWENT-ACC-NO: 2001-040814
DERWENT-WEEK: 200111

TITLE: Protection system of electronic document e.g. letter, enables or disables selected operations on file operating system or application program, based on communication from protection component at destination side

Basic Abstract Text (3):
USE - In e.g. internet, local area network (LAN) for protecting electronic documents including letters, specifications, control drawings, spread sheets, artwork, blue prints, video images output from scanners and routine business forms used for business and non-business applications in homes, offices.

Basic Abstract Text (4):
ADVANTAGE - Controls security of file by enabling or disabling the selected operational functionalities of the operating system and/or the application program at the destination side based on the communication from protection component, reliably. When the computer user accesses the protected file through the application program, the view of the file exhibiting all the enforced protection levels is provided to the user, thus preventing the user from generating duplicate copies of the entire or a portion of original content. The security information is embedded in the document by the flag in specific format, so that the flag is read by the operating system or application program to invoke specific restrictions on the operation that is performed on that document.

Basic Abstract Text (5):
DESCRIPTION OF DRAWING(S) - The figure shows schematic chart depicting electronic document protection system.

Standard Title Terms (1):
PROTECT SYSTEM ELECTRONIC DOCUMENT LETTER ENABLE DISABLE SELECT OPERATE FILE OPERATE SYSTEM APPLY PROGRAM BASED COMMUNICATE PROTECT COMPONENT DESTINATION SIDE

End of Result Set

Generate Collection | Print

L13: Entry 2 of 2 File: DWPI Jul 12, 2000

DERWENT-ACC-NO: 2000-425297
DERWENT-WEEK: 200175

TITLE: Personal identification related document used as transaction card security and imaging on transaction cards has printed region having given information on with second set of data derived from first set of data embedded in it

INVENTOR: HONSINGER, C W; RAY, L A

PATENT-ASSIGNEE: EASTMAN KODAK CO (EAST)

PRIORITY-DATA: 1998US-0218614 (December 22, 1998)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 1018712 A1	July 12, 2000	E	011	G07F007/10
US 6321981 B1	November 27, 2001		000	G06K005/00
JP 2000200337 A	July 18, 2000		007	G06K019/10
CN 1261705 A	August 2, 2000		000	G06K009/00

DESIGNATED-STATES: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
EP 1018712A1	November 24, 1999	1999EP-0203953	
US 6321981B1	December 22, 1998	1998US-0218614	
JP2000200337A	December 17, 1999	1999JP-0359294	
CN 1261705A	December 22, 1999	1999CN-0126500	

INT-CL (IPC): G06 K 5/00; G06 K 9/00; G06 K 17/00; G06 K 19/10; G07 F 7/10

ABSTRACTED-PUB-NO: EP 1018712A
BASIC-ABSTRACT:

NOVELTY - A machine readable information area has a first set of data stored in it. A printed region has information printed on it. The printed information has also embedded in it a second set of data derived from the first set of data.

DETAILED DESCRIPTION - Reading device (22) includes an image scanner (24) to translate the image printed on the printable region (14) into a digital image. The data from a reader (23) and the image scanner (24) are sent to a processor (26), which performs a secure hash algorithm on the data captured from the machine readable portion of a transaction card (10).

An INDEPENDENT CLAIM is included for:

(a) a method for producing a personal identification related document

USE - In transaction card security and imaging on transaction cards and other

personal identification related documents.

ADVANTAGE - Reduces fraudulent use of such documents, increased security features works with established transaction card procedures, eliminates the need for a clerk to verify the authenticity of a card by looking at an image or card protection feature, works with established transaction card procedures, such as the card validation value (CVV) by having the CVV as part of the data to be hashed, and for image verification values. May operate with unattended transaction terminals, such as ATM's and provide high levels of security while linking the printed transaction card with the machine readable data section, which includes embedded data that is invisible to a normal viewer.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic depiction of a personal identification related document reader system.

transaction card 10

printable region 14

reading device 22

reader 23

image scanner 24

processor 26

ABSTRACTED-PUB-NO: US 6321981B
EQUIVALENT-ABSTRACTS:

NOVELTY - A machine readable information area has a first set of data stored in it. A printed region has information printed on it. The printed information has also embedded in it a second set of data derived from the first set of data.

DETAILED DESCRIPTION - Reading device (22) includes an image scanner (24) to translate the image printed on the printable region (14) into a digital image. The data from a reader (23) and the image scanner (24) are sent to a processor (26), which performs a secure hash algorithm on the data captured from the machine readable portion of a transaction card (10).

An INDEPENDENT CLAIM is included for:

(a) a method for producing a personal identification related document

USE - In transaction card security and imaging on transaction cards and other personal identification related documents.

ADVANTAGE - Reduces fraudulent use of such documents, increased security features works with established transaction card procedures, eliminates the need for a clerk to verify the authenticity of a card by looking at an image or card protection feature, works with established transaction card procedures, such as the card validation value (CVV) by having the CVV as part of the data to be hashed, and for image verification values. May operate with unattended transaction terminals, such as ATM's and provide high levels of security while linking the printed transaction card with the machine readable data section, which includes embedded data that is invisible to a normal viewer.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic depiction of a personal identification related document reader system.

transaction card 10

printable region 14

reading device 22

reader 23

image scanner 24

processor 26

CHOSEN-DRAWING: Dwg.1/3

DERWENT-CLASS: T01 T04 T05
EPI-CODES: T01-J10B2; T04-D02; T04-D07C; T04-M; T05-D01A; T05-H02C5C;

End of Result Set

Generate Collection | Print

L13: Entry 2 of 2 File: DWPI Jul 12, 2000

DERWENT-ACC-NO: 2000-425297
DERWENT-WEEK: 200175

TITLE: Personal identification related document used as transaction card security and imaging on transaction cards has printed region having given information on with second set of data derived from first set of data embedded in it

Basic Abstract Text (6):
ADVANTAGE - Reduces fraudulent use of such documents, increased security features works with established transaction card procedures, eliminates the need for a clerk to verify the authenticity of a card by looking at an image or card protection feature, works with established transaction card procedures, such as the card validation value (CVV) by having the CVV as part of the data to be hashed, and for image verification values. May operate with unattended transaction terminals, such as ATM's and provide high levels of security while linking the printed transaction card with the machine readable data section, which includes embedded data that is invisible to a normal viewer.

Equivalent Abstract Text (6):
ADVANTAGE - Reduces fraudulent use of such documents, increased security features works with established transaction card procedures, eliminates the need for a clerk to verify the authenticity of a card by looking at an image or card protection feature, works with established transaction card procedures, such as the card validation value (CVV) by having the CVV as part of the data to be hashed, and for image verification values. May operate with unattended transaction terminals, such as ATM's and provide high levels of security while linking the printed transaction card with the machine readable data section, which includes embedded data that is invisible to a normal viewer.

L14: Entry 1 of 6 File: EPAB Aug 22, 2002

PUB-NO: WO002065353A1
DOCUMENT-IDENTIFIER: WO 2065353 A1
TITLE: COMMON WEB FACILITY FOR FRANCHISEE ONLINE SALES

PUBN-DATE: August 22, 2002

INVENTOR-INFORMATION:

NAME	COUNTRY
COOPER, ANDREW MCDONALD	AU
COOPER, TIMOTHY JOHN	AU

ASSIGNEE-INFORMATION:

NAME	COUNTRY
TOPSHOP HOLDINGS PTY LTD	AU
COOPER ANDREW MCDONALD	AU
COOPER TIMOTHY JOHN	AU

APPL-NO: AU00200165
APPL-DATE: February 15, 2002

PRIORITY-DATA: AU00PR313301A (February 15, 2001)

INT-CL (IPC): G06 E 17/60

ABSTRACT:

A web facility (10) allows a costumer to view a website (12) created by the facility (10), submit order information and make payment. The website (12) is displayed via costumer's web browser (11) utilising embedded data from both or either of a default database (13) and a linking database (14). The default database (13) is managed by the franchisor, licensor or main control body (15) of the website (12) and is used to provide generic web pages. The generic web pages may be modified by the content of the linking database (14) according to eligible franchisee costumer matching. The linking database (14) may be accessed by individual franchisees, licensees or authorised users (16) who manage or change the database's details including visual display elements, address details and so on which may be utilised in website (12).

DOCUMENT-IDENTIFIER: WO 2065353 A1
TITLE: COMMON WEB FACILITY FOR FRANCHISEE ONLINE SALES

Abstract Text (1):
A web facility (10) allows a costumer to view a website (12) created by the facility (10), submit order information and make payment. The website (12) is displayed via costumer's web browser (11) utilising embedded data from both or either of a default database (13) and a linking database (14). The default database (13) is managed by the franchisor, licensor or main control body (15) of the website (12) and is used to provide generic web pages. The generic web pages may be modified by the content of the linking database (14) according to eligible franchisee costumer matching. The linking database (14) may be accessed by individual franchisees, licensees or authorised users (16) who manage or change the database's details including visual display elements, address details and so on which may be utilised in website (12).

L14: Entry 4 of 6 File: DWPI Sep 5, 2000

DERWENT-ACC-NO: 2000-663963
DERWENT-WEEK: 200124

TITLE: Embedded data authentication method for digital audio, video and image data, involves embedding the authentication information in a pseudo-random fashion

INVENTOR: BARTON, J M

PATENT-ASSIGNEE: SONY CORP (SONY)

PRIORITY-DATA: 1994US-0357713 (December 14, 1994), 1997US-0824174 (March 26, 1997), 1998US-0193452 (November 17, 1998)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
US 6115818 A	September 5, 2000		016	H04L009/00

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
US 6115818A	December 14, 1994	1994US-0357713	Cont of
US 6115818A	March 26, 1997	1997US-0824174	Cont of
US 6115818A	November 17, 1998	1998US-0193452	
US 6115818A		US 5646997	Cont of
US 6115818A		US 5912972	Cont of

INT-CL (IPC): H04 L 9/00

RELATED-ACC-NO: 1997-363273;1999-417557 ;2000-338054 ;2000-593362 ;2001-233947

ABSTRACTED-PUB-NO: US 6115818A
BASIC-ABSTRACT:

NOVELTY - Arbitrary digital information is embedded using any encryption technique within a stream of digital data, in a way that avoids detection by a casual observer and allows a user to determine whether the digital data have been modified from their intended form. The embedded information may only be extracted as authorized and may be used to verify that the digital data stream has been modified.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a method for extracting a bit string authentication from a digital block.

USE - For digital audio, video and image data.

ADVANTAGE - Encryption can be used to enhance authentication capability and can prevent loss of revenue by unauthorized copying.

DESCRIPTION OF DRAWING(S) - The figure is a block schematic diagram of an authentication system.

ABSTRACTED-PUB-NO: US 6115818A
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg [redacted]

DERWENT-CLASS: W01
EPI-CODES: W01-A05; W01-A05A;

L14: Entry 4 of 6 File: DWPI Sep 5, 2000

DERWENT-ACC-NO: 2000-663963
DERWENT-WEEK: 200124

TITLE: Embedded data authentication method for digital audio, video and image data, involves embedding the authentication information in a pseudo-random fashion

Basic Abstract Text (1):
NOVELTY - Arbitrary digital information is embedded using any encryption technique within a stream of digital data, in a way that avoids detection by a casual observer and allows a user to determine whether the digital data have been modified from their intended form. The embedded information may only be extracted as authorized and may be used to verify that the digital data stream has been modified.

Standard Title Terms (1):
EMBED DATA AUTHENTICITY METHOD DIGITAL AUDIO VIDEO IMAGE DATA EMBED AUTHENTICITY INFORMATION PSEUDO RANDOM FASHION

L14: Entry 5 of 6 File: DWPI Nov 4, 1998

DERWENT-ACC-NO: 1998-559663
DERWENT-WEEK: 199904

TITLE: Key management system e.g. for smart cards - has file decryption key not stored on card which is generated and stored in remote data centre which is only accessible by authorised user

INVENTOR: SCOLNICK, M J

PATENT-ASSIGNEE: PITNEY BOWES INC (PITB)

PRIORITY-DATA: 1997US-0810057 (March 4, 1997)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 875868 A2	November 4, 1998	E	012	G07F007/10
CA 2231210 A	September 4, 1998		000	G06K019/073

DESIGNATED-STATES: AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SI

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
EP 875868A2	March 4, 1998	1998EP-0103815	
CA 2231210A	March 3, 1998	1998CA-2231210	

INT-CL (IPC): G06 K 19/073; G07 F 7/10

ABSTRACTED-PUB-NO: EP 875868A
BASIC-ABSTRACT:

The system comprises a variable encryption code embedded in a data file in the storage medium of a smart card. An information terminal is configured for reception of the smart card. A data centre remote from the information terminal electronically connects with the information terminal, the data centre includes a file decryption key capable of deciphering the variable encryption code of the smart card, so the data centre electronically transmits the file decryption key to the smart card when the smart card is received in the information terminal and the information terminal is electronically connected to the data centre so the file decryption key enables the information terminal to access stored data in the data file of the smart card.

The data centre assigns another variable encryption code and deciphering file decryption key for the data file of the smart card and to transmit another variable encryption code to the information terminal when access is sought for the data file of the smart card so the another variable encryption code is unique relative to the variable encryption code.

ADVANTAGE - Prevents unauthorised retrieval of personal information stored on smart card. Provides improved data retrieval system for accessing personal information stored on smart card.

ABSTRACTED-PUB-NO: EP 875868A

EQUIVALENT-ABSTRACTS

CHOSEN-DRAWING: Dwg.1/4

DERWENT-CLASS: S05 T01 T04 T05
EPI-CODES: S05-G02G; T01-D01; T01-H01C1; T04-K; T05-D01A; T05-H02C;

DERWENT-ACC-NO: 1998-559663
DERWENT-WEEK: 199904

TITLE: Key management system e.g. for smart cards - has file decryption key not stored on card which is generated and stored in remote data centre which is only accessible by authorised user

Basic Abstract Text (1):
The system comprises a variable encryption code embedded in a data file in the storage medium of a smart card. An information terminal is configured for reception of the smart card. A data centre remote from the information terminal electronically connects with the information terminal, the data centre includes a file decryption key capable of deciphering the variable encryption code of the smart card, so the data centre electronically transmits the file decryption key to the smart card when the smart card is received in the information terminal and the information terminal is electronically connected to the data centre so the file decryption key enables the information terminal to access stored data in the data file of the smart card.

Standard Title Terms (1):
KEY MANAGEMENT SYSTEM SMART CARD FILE DECRYPTER KEY STORAGE CARD GENERATE STORAGE REMOTE DATA CENTRE ACCESS AUTHORISE USER

End of Result Set

Generate Collection | Print

L14: Entry 6 of 6 File: DWPI Nov 27, 1997

DERWENT-ACC-NO: 1998-018703
DERWENT-WEEK: 199950

TITLE: Embedding auxiliary data into host digital image data noise - selecting block of values having centre and first offset value obtained from centre of block, and replacing data with second block offset determined from auxiliary data, and retrieving embedded data using digital key

INVENTOR: ETTINGER, J M; HANDEL, T G ; SANDFORD, M T

PATENT-ASSIGNEE: ETTINGER J M (ETTII), HANDEL T G (HANDI), SANDFORD M T (SANDI), UNIV CALIFORNIA (REGC)

PRIORITY-DATA: 1996US-0646837 (May 8, 1996)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
WO 9744725 A2	November 27, 1997	E	034	G06F000/00
US 5970140 A	October 19, 1999		000	H04N007/167
AU 9732042 A	December 9, 1997		000	G06F011/00

DESIGNATED-STATES: AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN AT BE CH DE DK EA ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
WO 9744725A2	May 8, 1997	1997WO-US07902	
US 5970140A	May 8, 1996	1996US-0646837	
AU 9732042A	May 8, 1997	1997AU-0032042	
AU 9732042A	WO 9744725		Based on

INT-CL (IPC): G06 F 0/00; G06 F 11/00; H04 N 7/167

ABSTRACTED-PUB-NO: US 5970140A
BASIC-ABSTRACT:

The method selects values from the digital host data in a sequence determined by a digital key, and creates a digital representation of the auxiliary data in the form of a sequence of individual bit values. From the host data is selected a block of data values with a centre and first offset value obtained from the centre of the block (128).

The individual host data values are replaced with a second block offset value determined from the auxiliary data. The replacement values are outputted with the auxiliary data embedded into a file format specified for the digital host data.

USE - Relates to digital manipulation of numerical data in which low order bits are modified without affecting meaning and contents of numerical data.

ADVANTAGE - Reduces error caused by added information and thwarts unauthorised access to information embedded into host data. Allows authorised extraction of embedded data from digital information stream. doubles amount of auxiliary data added to host data values compared to bit replacement methods for high bit rate coding.

ABSTRACTED-PUB-NO: WO 9744725A
EQUIVALENT-ABSTRACTS:

The method selects values from the digital host data in a sequence determined by a digital key, and creates a digital representation of the auxiliary data in the form of a sequence of individual bit values. From the host data is selected a block of data values with a centre and first offset value obtained from the centre of the block (128).

The individual host data values are replaced with a second block offset value determined from the auxiliary data. The replacement values are outputted with the auxiliary data embedded into a file format specified for the digital host data.

USE - Relates to digital manipulation of numerical data in which low order bits are modified without affecting meaning and contents of numerical data.

ADVANTAGE - Reduces error caused by added information and thwarts unauthorised access to information embedded into host data. Allows authorised extraction of embedded data from digital information stream. doubles amount of auxiliary data added to host data values compared to bit replacement methods for high bit rate coding.

CHOSEN-DRAWING: Dwg.1/12

DERWENT-CLASS: T01
EPI-CODES: T01-D01; T01-J10G;

End of Result Set

L14: Entry 6 of 6 File: DWPI Nov 27, 1997

DERWENT-ACC-NO: 1998-018703
DERWENT-WEEK: 199950

TITLE: Embedding auxiliary data into host digital image data noise - selecting block of values having centre and first offset value obtained from centre of block, and replacing data with second block offset determined from auxiliary data, and retrieving embedded data using digital key

Basic Abstract Text (4):
ADVANTAGE - Reduces error caused by added information and thwarts unauthorised access to information embedded into host data. Allows authorised extraction of embedded data from digital information stream. doubles amount of auxiliary data added to host data values compared to bit replacement methods for high bit rate coding.

Equivalent Abstract Text (4):
ADVANTAGE - Reduces error caused by added information and thwarts unauthorised access to information embedded into host data. Allows authorised extraction of embedded data from digital information stream. doubles amount of auxiliary data added to host data values compared to bit replacement methods for high bit rate coding.

Standard Title Terms (1):
EMBED AUXILIARY DATA HOST DIGITAL IMAGE DATA NOISE SELECT BLOCK VALUE CENTRE FIRST OFFSET VALUE OBTAIN CENTRE BLOCK REPLACE DATA SECOND BLOCK OFFSET DETERMINE AUXILIARY DATA RETRIEVAL EMBED DATA DIGITAL KEY

L19: Entry 1 of 2 File: PGPB Dec 26, 2002

PGPUB-DOCUMENT-NUMBER: 20020196285
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020196285 A1

TITLE: Graphical program node for accessing capabilities of a software object

PUBLICATION-DATE: December 26, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Sojoodi, Omid	Austin	TX	US	
Dye, Robert	Austin	TX	US	
Parthasarathy, Murali	Austin	TX	US	
Kudukoli, Ram	Austin	TX	US	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
National Instruments Corporation				02

APPL-NO: 10/ 158724 [PALM]
DATE FILED: May 30, 2002

RELATED-US-APPL-DATA:
Application 10/158724 is a continuation-of US application 09/136123, filed August 18, 1998, US Patent No. 6437805
Application 10/158724 is a continuation-of US application 08/916005, filed August 21, 1997, US Patent No. 6102965
Application 08/916005 is a continuation-in-part-of US application 08/810079, filed March 4, 1997, US Patent No. 6064812
Application 08/810079 is a continuation-in-part-of US application 08/717771, filed September 23, 1996, US Patent No. 5847953
Application is a non-provisional-of-provisional application 60/056528, filed August 21, 1997,

INT-CL: [07] G09 G 5/00

US-CL-PUBLISHED: 345/771
US-CL-CURRENT: 345/771

REPRESENTATIVE-FIGURES: 3

ABSTRACT:

A system and method for creating a graphical program, wherein the graphical program is operable to access capabilities of an object. During creation of the graphical program, the user operates to place an object node in the graphical program, wherein the object node is operable to access capabilities of the object. This preferably includes the user arranging on the screen the graphical program, including the object node and various other nodes, and connecting the various nodes to create the graphical program. The user then configures the object node to receive information on the object, preferably by the user configuring the object node with a reference to the object, e.g., a pointer, address, or other information which specifies the identity and/or location of the object. The user also selects one or more methods to

be invoked on the object and/or one or more properties to get/set on the object. Once the graphical program has been created, then during execution of the graphical program, the object node accesses the capabilities of the object.

CONTINUATION DATA

[0001] This is a continuation of patent application Ser. No. 09/136,123 titled System and Method for Accessing Object Capabilities in a Graphical Program" filed on Aug. 18, 1998, whose inventors are Omid Sojoodi, Robert Dye, Murali Parthasarathy and Ram Kudukoli, which claims benefit of U.S. Provisional Application No. 60/056,528 titled "System and Method for Providing Automation Server Capabilities in Graphical Programs," by Ram Kudukoli, Robert Dye and Murali Parthasarathy, filed on Aug. 21, 1997.

[0002] This is a continuation of patent application Ser. No. 09/136,123 titled System and Method for Accessing Object Capabilities in a Graphical Program" filed on Aug. 18, 1998, whose inventors are Omid Sojoodi, Robert Dye, Murali Parthasarathy and Ram Kudukoli, which is a continuation-in-part of co-pending patent application Ser. No. 08/916,005 titled "System and Method for Providing Client/Server Access to Graphical Programs" filed on Aug. 21, 1997, whose inventors were Robert Dye and Omid Sojoodi, now U.S. Pat. No. 6,102,965, which is a continuation in part of co-pending patent application Ser. No. 08/810,079 titled "System and Method for Developing Automation Clients using a Graphical Data Flow Program" filed on Mar. 4, 1997, whose inventors were Murali Parthasarathy and Omid Sojoodi, now U.S. Pat. No. 6,064,812, which is a continuation-in-part of co-pending application Ser. No. 08/717,771 titled "System and Method for Performing Class Checking of Objects in a Graphical Data Flow Program" and filed Sep. 23, 1996, whose inventors were Omid Sojoodi and Stephen W. Rogers, now U.S. Pat. No. 5,847,953.

[0003] This is a continuation of patent application Ser. No. 09/136,123 titled System and Method for Accessing Object Capabilities in a Graphical Program" filed on Aug. 18, 1998, whose inventors are Omid Sojoodi, Robert Dye, Murali Parthasarathy and Ram Kudukoli, which is a continuation in part of co-pending patent application Ser. No. 08/810,079 titled "System and Method for Developing Automation Clients using a Graphical Data Flow Program" filed on Mar. 4, 1997, whose inventors were Murali Parthasarathy and Omid Sojoodi, now U.S. Pat. No. 6,064,812, which is a continuation-in-part of co-pending application Ser. No. 08/717,771 titled "System and Method for Performing Class Checking of Objects in a Graphical Data Flow Program" and filed Sep. 23, 1996, whose inventors were Omid Sojoodi and Stephen W. Rogers, now U.S. Pat. No. 5,847,953.

[0004] This is a continuation of patent application Ser. No. 09/136,123 titled System and Method for Accessing Object Capabilities in a Graphical Program" filed on Aug. 18, 1998, whose inventors are Omid Sojoodi, Robert Dye, Murali Parthasarathy and Ram Kudukoli, which is a continuation-in-part of co-pending application Ser. No. 08/717,771 titled "System and Method for Performing Class Checking of Objects in a Graphical Data Flow Program" and filed Sep. 23, 1996, whose inventors were Omid Sojoodi and Stephen W. Rogers, now U.S. Pat. No. 5,847,953.

CROSS-REFERENCE TO RELATED APPLICATIONS

[0005] The following applications are related to the present application:

[0006] U.S. patent application Ser. No. 08/916,005 titled "System and Method for Providing Client/Server Access to Graphical Programs" filed on Aug. 21, 1997, whose inventors were Robert Dye and Omid Sojoodi (Atty. Dkt. No. 5150-25400);

[0007] U.S. patent application Ser. No. 08/810,079 titled "System and Method for Developing Automation Clients using a Graphical Data Flow Program" filed on Mar. 4, 1997, whose inventors were Murali Parthasarathy and Omid Sojoodi, (Atty. Dkt. No. 5150-18300),

[0008] U.S. patent application Ser. No. 08/811,187 titled "System and Method for Performing Class Propagation and Type Checking in a Graphical Automation Client" and filed on Mar. 4, 1997, whose inventors were Murali Parthasarathy and Omid Sojoodi, (Atty. Dkt. No. 5150-18400),

[0009] U.S. patent application Ser. No. 08/717,771 titled "System and Method for Performing Class Checking of Objects in a Graphical Data Flow Program" (Atty. Dkt.

No. 5150-16900) and [redacted]led Sep. 23, 1996, whose inven[redacted]s were Omid Sojoodi and Stephen W. Rogers.

[0010] U.S. patent application Ser. No. 08/717,772 titled "System and Method for Performing Interface Independent Virtual Instrumentation Functions Using Attribute Nodes in a Graphical Data Flow Program" (Atty. Dkt. No. 5150-17000) and filed Sep. 23, 1996, whose inventors were Omid Sojoodi and Stephen W. Rogers.

DOCUMENT-IDENTIFIER: US 20020196285 A1
TITLE: Graphical program node for accessing capabilities of a software object

Summary of Invention Paragraph (2):
[0011] A portion of the disclosure of this patent document contains material to which a claim of copyright protection is made. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but reserves all other rights whatsoever.

Summary of Invention Paragraph (16):
[0025] An example of a server is Microsoft Excel.RTM., which exports its objects for use by clients. An example of an object technology is Active X, formerly called OLE (Object Linking and Embedding), promulgated by Microsoft. For example, the Microsoft Excel spreadsheet program, the Microsoft Access.RTM. database program, and the Microsoft Word.RTM. word processing program, all export objects using the Active X interface. Active X is an industry standard object or component interface used by application programs to provide objects in a consistent manner to other application programs, development tools, and macro languages. Other examples of object technologies are OpenDoc.RTM. and the Common Object Request Broker Architecture (CORBA).

Brief Description of Drawings Paragraph (16):
[0048] FIG. 11 is a screen shot illustrating an exemplary list of the type libraries associated with the OLE Automation servers present in a system;

Detail Description Paragraph (76):
[0155] Preferably, the automation control 274 comprises a draw method which the front panel editor 262 and block diagram editor 264 invoke in order to display an automation control icon in the front panel and to display an automation refnum icon in the block diagram, respectively. FIG. 8 shows an automation refnum displayed in a block diagram. FIG. 8 also shows a pop-up menu for the automation refnum including a "Select OLE Class" menu item with a "Browse" item. Preferably, the user right clicks a mouse on the automation refnum in order to see the pop-up menu.

Detail Description Paragraph (79):
[0158] Referring again to FIG. 8a, in response to user input, the automation refnum queries the object manager 268 for a list of type libraries 270 (of FIG. 3) associated with the automation servers present in the system. The automation refnum displays the list of type libraries 270 associated with the automation servers in step 386. Preferably, the object manager 268 provides the automation refnum with a list of OLE Automation type libraries in the system. In one embodiment, the object manager 268 provides the automation refnum with a list of type libraries for each automation technology in the system.

Detail Description Paragraph (80):
[0159] Preferably, the user input includes the user clicking on the "Browse" item of the "Select OLE class" item of the automation refnum pop-up menu, shown in FIG. 12, and selecting the pull-down menu in the "Type Library" window shown in FIG. 12. Preferably, the object manager 268 queries the Windows Registry to obtain a list of OLE Automation type libraries present in the system. Preferably, the automation refnum displays the type libraries associated with the OLE Automation servers present in the system, as shown in FIG. 11. In one embodiment, the automation refnum displays the type libraries associated with the automation technology which was selected in step 384.

Detail Description Paragraph (92):
[0169] The <size>byte of the type descriptor is as described above. The <refnumCode>is the type code for a refnum. The <AutoRefnumKind>value distinguishes this refnum from other refnums as an automation refnum. The <AutomationType>indicates the OLE automation type, such as the <kStOLEAutoType>value which indicates a static OLE automation type. The <no of int16's>field indicates the number of 16 bit words which follow. The <kCoClassCLSID>value indicates the following 128 bits are a class identifier. The <CLSID of created object>is a unique 128 bit number associated with the particular automation class which the automation refnum references. The <kTypeLibCLSID>value indicates the following 128 bits are a type library identifier. The <CLSID of type library>is a unique 128 bit number associated with the particular type library to which the automation class belongs. The <DISPID>is a Dispatch ID, which is a long integer which uniquely specifies a class within a type library. The Dispatch ID is associated with the Microsoft IDispatch interface for dispatch methods and properties. The Dispatch ID is unique within a type library. In the example shown in FIG. 11, the type descriptor provided by the automation refnum includes information to specify the Microsoft "Excel" automation application type library and the "Application" automation class.

Detail Description Paragraph (140):
[0217] The first automation node has a first automation class and the second automation node has a second automation class. The first and second automation classes may be the same or different. The automation class of each of the first and second automation nodes is set either by default when the automation node is dropped or directly by the user, preferably using the "Select OLE Class" item in the automation node pop-up menu, as shown in FIG. 30 In response to a user wiring the first and second automation nodes together, the block diagram editor 264 displays a wire connecting the refnum output terminal of the first automation node to the refnum input terminal of the second automation node in step 544. In response to the user wiring the first and second automation nodes together, the automation class of the first automation node is propagated to the second automation node in step 546. That is, the second automation node receives the first automation class in the type descriptor from the first automation node and changes the automation class of the second automation node to the first automation class if the second automation class is different from the first automation class.

Detail Description Paragraph (144):
[0221] The first and second automation nodes have a first automation class. The automation class of each of the first and second automation nodes is set either by default when the automation node is dropped or directly by the user, preferably using "Select OLE Class" item in the automation node pop-up menu, as shown in FIG. 30. In addition, the automation class of the automation nodes may have previously been set via the class propagation steps described in the flowcharts of FIG. 22 or FIG. 26.

Detail Description Paragraph (372):
[0449] The ActiveX container manipulates data on ActiveX objects. These changes are preferably displayed in the container on the front panel. This container allows the user to use ActiveX controls and embed documents on the front panel.

End of Result Set

Generate Collection | Print

L19: Entry 2 of 2 File: PGPB Aug 15, 2002

PGPUB-DOCUMENT-NUMBER: 20020112093
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020112093 A1

TITLE: Method of processing information embedded in a displayed object

PUBLICATION-DATE: August 15, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Slotznick, Benjamin	Mt. Gretna	PA	US	

APPL-NO: 09/ 974132 [PALM]
DATE FILED: October 9, 2001

RELATED-US-APPL-DATA:
Application is a non-provisional-of-provisional application 60/238908, filed October 10, 2000,

INT-CL: [07] G06 F 9/46, G06 F 9/00

US-CL-PUBLISHED: 709/329
US-CL-CURRENT: 709/329

REPRESENTATIVE-FIGURES: 2A

ABSTRACT:

Information embedded in a displayed object is transferred from one browser window to another. Each of the browser windows display a Web page. The object is displayed on one of the Web pages and, by "dragging" and "dropping" the embedded information to the other Web page, a function is performed on the embedded information, such as one that converts text associated with the embedded information into an audible output. A user who has difficulty reading text displayed on a Web page can click on an image embedded in the text, or drag and drop the information embedded in the displayed image to another Web page used to perform the conversion function.

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/238,908, filed Oct. 10, 2000, entitled "A METHOD OF USER TRANSFER OF INFORMATION FROM ONE WEB PAGE TO ANOTHER AND USER ACCESS TO TEXT INFORMATION THAT THE USER HAS DIFFICULTY READING."

End of Result Set

Generate Collection | Print

L19: Entry 2 of 2 File: PGPB Aug 15, 2002

DOCUMENT-IDENTIFIER: US 20020112093 A1
TITLE: Method of processing information embedded in a displayed object

Summary of Invention Paragraph (2):
[0002] Portions of the documentation in this patent document contain material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office file or records, but otherwise reserves all copyright rights whatsoever.

Detail Description Paragraph (18):
[0035] In an alternative embodiment of the invention, different images are used with the embedded data. For example, the Haptek animations will change shape when given certain function calls, such as changing the shape of the animated head from a dog to a cat, or from a woman to a man. In the alternative embodiment, one image (e.g. an image of a cat) contains the function call to change the head to a cat's. Another image (e.g. the image of a man) contains the function call to change the head to a man's. Dragging the various images to the target window causes the head to change in accordance with the embedded data in the image. Of course, multiple arguments in the embedded data could have the head change to a specific shape and speak specific words. For example, dragging and dropping a cat image might cause the head to change to the shape of a cat and speak the words "Meow meow" whereas dragging and dropping a man image might cause the head to change to the shape of a man and speak the words "Let's watch football and drink some beer." The programmer who codes Web page 2 decides what actions can be controlled by the author of Web page 1, although the author of Web page 1 may have considerable choices.

Detail Description Paragraph (45):
[0062] Referring now to FIG. 2B, the drag and drop operation is implemented as follows. First the user places the computer cursor over the displayed object in the first Browser Window that has the embedded caption (step 214). Next, the user depresses the left mouse button while keeping the computer cursor over the displayed object to capture the information embedded in the displayed object (step 216). This causes the computer's operating system to store the function call, including the text of the link (more specifically, the text specified as the href data in the link), into the short term memory associated with an OLE object (step 218). (OLE objects are specific to the Windows operating system although other operating systems recognize similar objects and treat them in similar or analogous manners.) The user continues the drag and drop (transfer) operation by keeping the left mouse button depressed and moving the cursor over to a target area, which in this case is the second Browser Window (step 220). The user then releases the left mouse button, while keeping the computer cursor over the second Browser Window (step 222). Releasing the left mouse button causes the operating system to send a message that an OLE object has been "dropped" (released) at the cursor location, which in this case is in the second Browser Window 2. The message indicates to various active programs running in the second Browser Window that the embedded information has been released (step 224).

Detail Description Paragraph (46):
[0063] Referring now to FIG. 2C, Web page 2, as previously described, contains JavaScript codes which will execute the SpeakCaption function. The browser continually monitors whether any messages are sent by the operating system to which it must respond or on which it must act (step 230). In particular, the browser monitors whether any messages have been sent from the operating system providing

notice that an OLE "link" object has been dropped into the window in which the browser is operating, which in this case is the second Browser Window. When the browser in the second Browser Window detects that an OLE link object has been dropped onto the window by receiving the message sent from the operating system (step 232), the browser retrieves the function call (e.g., href data, link text) from the OLE object short term memory (step 234). Next, the browser determines whether the function call has href data with a JavaScript function (step 236). If so, the browser will attempt to evaluate and execute the function. If it is determined that the function is a SpeakCaption function (step 238), the browser will load the text (a character string) that makes up the argument of the SpeakCaption function into a plug-in program (e.g., Haptek plug-in) (step 240). The text contains commands for the animated head to execute (turn, change shape, speak text), which the plug-in program will implement and execute (step 242). Then the process proceeds back to step 230, where the second Browser Window awaits more captions to be dragged and dropped onto it.

InfoWorld
Dec 21, 1998

VirusNet packs key scanning tools.(Safetynets' VirusNet PC and VirusNet LAN 3.0 anti-virus software)(Software Review)(Evaluation)

Author/s: Stuart Mcclure

Best known for its StopLight security products, SafetyNet also boasts the detection of more than 22,500 viruses and Trojan programs in its latest VirusNet PC and VirusNet LAN 3.0 releases. The duo's comprehensive store of signatures and small footprint make it worth considering as a low-cost anti-virus solution for small to midsize LANs.

Although I could not confirm the accuracy rate for the 22,500 virus-scanning capabilities, I did find the products to be capable of detecting most of the tough viruses I threw at it -- including Armageddon, Silly/Zany, Burger, Better World, Intruder, and others. VirusNet's compact size is an advantage compared to its resource-intensive rivals, yet it is hampered by some usability limitations in its current form.

Detection strengths

In my tests, VirusNet also detected viruses in all .zip files scanned. The product recursively uncompresses and scans nested .zip and .ajr files as well. Malicious virus writers will often bury virus executables in nested, compressed files as a way to avoid detection. Yet surprisingly, some older versions of Norton AntiVirus, for example, stopped at scanning the first .zip file -- missing the nested .zip files.

With the recent release of dangerous Trojan programs such as BackOrifice and Netbus (see "Netbus hacker tool presents a greater threat to Windows shops than BackOrifice," Dec. 14, page 67), I am especially interested in seeing which anti-virus programs can accurately detect these new Trojans. During a scan of our systems, VirusNet accurately found both BackOrifice and Netbus. The BackOrifice file boserve.exe and the Netbus files patch.exe and netbus.exe were found in multiple .zip files -- even with the names changed. VirusNet accomplishes this through checksums: It compares the checksum of the file with its checksum database of viruses and Trojans.

Although new OLE viruses are growing in popularity, their detection and cleanup can be difficult. VirusNet does provide this level of detection with its compound document logic technology. Using

Microsoft's own .dll files. This technology lets the virus-scanning engine peer inside the document to find an embedded object and scan for viruses.

One of VirusNet's extras is its capability to scan for boot and master boot record viruses in files you may have downloaded from your virus-exchange travels. Also new are Java-class scanning and Java heuristics capabilities, but as Safetynet officials admit, only one Java virus currently exists, and it's only in the lab.

Compact but limited

VirusNet's size is one of its biggest advantages: It only requires approximately 1.5MB, so it can be installed on laptops and underpowered desktops that can't be upgraded. Just try installing Network Associates' VirusScan or Symantec's Norton AntiVirus -- which require from 4MB to 24MB -- on one of your older 486es and you will appreciate VirusNet's economy.

However, VirusNet's usability is somewhat limited when compared to its rivals. For example, VirusNet does not include the right-mouse click in Explorer or folder views for file and directory scanning that Norton or VirusScan provide. VirusNet 2.0 had this capability, but because of time restraints, Version 3.0 was shipped without this functionality. According to SafetyNet officials, Version 3.1 will add the right-mouse-click scanning back.
Another limitation is the fact that VirusNet can't selectively scan multiple subdirectories in the GUI console; it can scan only those within a parent directory. Yet the DOS version -- vn.exe -- does allow for selective subdirectory scanning. Also missing are password-protection features to keep users from tinkering with settings you have made.

The monitoring capabilities provided are all standard, including floppy boot-sector scanning, monitoring of scan conditions, and deciding what actions to take when a virus is detected. Although none of these features will knock your socks off, they are all critical to anti-virus functionality.

Management help

The VirusNet LAN component provides valuable centralized management of the workstation agents -- essential for any network manager. Log-in scripts in NetWare and Windows NT will allow you to automatically load the agent software for the clients and handle central management through the LAN Management Console.

You can also schedule scanning events for your network with VirusNet LAN's simple task scheduler. Simply set a scan frequency and time to automatically scan your servers and users' hard drives.

The VirusNet duo gives you all the core components of a solid network anti-virus product, but keep an eye out for expanded functionality and usability as it matures.

Stuart McClure (stuart.mcclure@ey.com), co-author of InfoWorld's Security Watch column, is a senior manager at Ernst & Young Security Services, in Palo Alto, Calif.

THE BOTTOM LINE: GOOD

VirusNet PC, VirusNet LAN 3.0

Safetynet's upgrades to its capable anti-virus tools -- VirusNet PC and VirusNet LAN 3.0 -- are worth a look, thanks to useful extras and a small footprint.

Pros: Compound document logic for scanning OLE embedded viruses; scanning of nested .zip files; detection of Netbus and BackOrifice Trojan programs; Java-class scanning; monitoring agents; automatic viral-pattern updates; small footprint.

Cons: Some usability issues and limitations.

Safetynet Inc., Springfield, N.J.; (800) 672-7233; fax: (973)-467-1611; info@safetynet.com; www.safetynet.com.

Price: $59.99 per license.

Platforms: DOS, Windows 3.x, Windows 95, Windows 98, Windows NT.

Telecomworldwire
Nov 9, 1999

-New groupware system launched by MC2/SoftArc.(FirstClass Intranet Server Gold from MC2 Learning Systems and SoftArc International)(Brief Article)(Product Announcement)

TELECOMWORLDWIRE-(C) 1994-9 M2 COMMUNICATIONS LTD

MC2 Learning Systems Inc/SoftArc International has launched FirstClass Intranet Server Gold, its new groupware system. In addition to calendaring, post office mirroring and online back-up, the system offers a new audio, conference and e-mail feature. ACE-mail allows users to select the most appropriate communications medium for their requirements - e-mail for personal and individual communication, c-mail for group collaboration and discussion in online virtual 'conferences' and a-mail for the sending, receiving, playing and storing of audio and video files. Other features include compound document editing - an ability to insert graphics files into e-mail - and support for up to 250,000 users. Availability and pricing were not disclosed.

Information Today
Dec, 2001

File NET, arbortext team to develop cross-media publishing solution. (Internet publishing today).
Author/s:

FileNET Corp. and Arbortext (http://www.arbortext.com) have announced a partnership to integrate FileNET's Panagon family of enterprise content-management products with Arbortext's Epic software. The two companies are working together to combine Panagon's process-management and enterprise content-management services with Arbortext's XML-based authoring, conversion, and multichannel publishing of customized documents. With the integration, customers will be able to create content once and repackage and deliver that content for multiple audiences and multiple types of media.

According to the announcement, FileNET and Arbortext will help customers quickly access specific information to re-purpose and deliver that information in a variety of applications. Customers will be able to create documents that leverage content created in many disparate forms and bring this content together to deliver fresh, consistent, and complete information to multiple types of media, including Adobe PDF, the Web, CD-ROM, and wireless devices.

Panagon's eProcess capability adds the automation factor to the planned end-to-end solution. For example, in a product launch application, multiple authors can use Arbortext's Epic Editor to collaboratively create an XML document containing all of the content critical to the release of a new product. The XML document can then be separated or "burst" into multiple components based on their reuse requirements. The individual components of the compound document, such as product descriptions, installation instructions, warranty statements, pricing, and support policies, are packaged as needed and can be automatically routed to the appropriate function within the organization (sales, order processing, inventory control, customer service, and accounting) as well as to corporate Web sites. Arbortext's XML publishing enforces the document structure, defines the bursting blueprint, and enables publishing into the appropriate format (HTML, Adobe PDF, WML, and others). According to the announcement, FileNET's Panagon e Process automates this procedure, saving time, eliminating costly mistakes, and ensuring appropriate content delivery.

FileNET and Arbortext will also offer other systematic and repeatable applications, such as dynamic catalogs, on-the-fly insurance-policy

generation, complex p[redacted]shing, policies and procedures, secu[redacted]s research, and automated portfolio generation.

Sue Feldman, director of content and retrieval technologies at IDC, believes that the partnership effectively addresses business applications that require complex document creation and publishing support. "The purpose of content management and retrieval is to deliver the right information to the right person at the right time. Increasingly, this means that information must be pulled from all over the enterprise, personalized for the role and interests of the recipient, and delivered to the appropriate device. Large documents that have multiple authors, experience frequent updates, or require a high degree of navigation often create complex management problems. If we add to that the need to show some information to one group of recipients but not to another, the management problems are compounded still further. The Arbortext capabilities provide access to structured information within the FileNET repository on a more granular basis than the whole document, resulting in more intelligent documents that can be a ssembled and reformatted to address different purposes or audiences."

PR Newswire
April 7, 2000

ESPS Announces Compatibility of its CoreDossier(R) Assembly and Publishing Software With Lotus Notes/Domino.

Integration of Two Products Offers Additional Functionality for Managing
Complex Publications

FORT WASHINGTON, Pa., Feb. 29 /PRNewswire/ --

ESPS, Inc. (Nasdaq: ESPS), the premier provider of business-to-business software and expertise that accelerate the assembly and publishing of business-critical knowledge, today announced the integration of its CoreDossier(R) software (Version 4.x) with the Lotus Notes/Domino repository. The integration offers users enhanced functionality for managing complex publications. Lotus Development Corp. develops, markets and supports the Domino family of integrated messaging and Web application software platform products for growing companies that need to improve customer responsiveness and streamline business processes.

The ESPS CoreDossier software suite is used by organizations worldwide to efficiently plan, assemble, manage, publish and share mission-critical business information, thus reducing the time and costs associated with these efforts. CoreDossier publishes to the Internet, corporate intranets, directly to paper or to industry-specific standards in formats like HTML, XML, PDF and TIFF. The output generated from CoreDossier can quickly and effectively be consumed by the business user community either electronically or on paper. Faster and more effective business decisions, improved time-to-market for new products, and achieving regulatory compliance are examples of key benefit gains.

CoreDossier functions with Lotus Notes/Domino to allow users to create and manage cohesive, complex publications with mixed content sources stored in Domino databases. Examples of mixed content could include Notes form data, attachments (such as Microsoft Word documents, Microsoft Excel documents, and TIFF) and embedded OLE objects. Specific integration features include the ability to:

-- Navigate databases, view folders, categories, and documents to add

Notes content, including form data, attachments and embedded OLE

objects, as source documents into CoreDossier publications

-- Transform more than 130 source file formats into PDF renditions with

automatic check-in of the rendition into a Lotus Notes rendition

database

-- Use Lotus Notes to store CoreDossier tables of content

-- Merge document meta data from Lotus Notes with published output

-- Check-in published output to a Lotus Notes/Domino database

automatically

-- Batch check-in of file system documents

"Lotus enjoys the largest user installation base in the document and content management industry," said Lawrence Spoerl, director of worldwide alliances at ESPS. "CoreDossier's robust assembly features provide needed productivity gains to most corporate publishing needs. Our single interface, multiple source document access capability continues to expand and reach more and more users."

Since its introduction in 1995, CoreDossier(R) has set the standard in electronic regulatory and business-compliance publishing, with customers in the pharmaceutical, biotech, chemical and utilities industries. Also, ESPS, with its CoreDossier software, has been first to market with Web-based product registrations and other Internet publishing solutions.

About ESPS

ESPS, Inc. provides business-to-business software and expertise that accelerate the planning, assembling, managing, publishing, and sharing of business-critical knowledge for paper, portals and the Web. Since 1995, ESPS has been the leading developer of solutions that address the needs of companies faced with compound document publishing requirements through the application of industry expertise, advanced technology and a commitment to high-quality implementations. The ESPS world headquarters is located in suburban Philadelphia, with additional offices throughout North America and in Europe. More information can be found at www.esps.com, or by reaching the Company at 800-515-ESPS (North America) or +44 (0) 1753 725203 (Europe).

The statements in this news release which are not historical facts are forward-looking statements. These forward-looking statements involve risks and uncertainties that could render them materially different, including, but not limited to, the effect of fluctuations in the Company's operating results, the Company's reliance on a limited number of significant customers, the Company's reliance on the CoreDossier product family, the Company's ability to market and sell its products and services in its targeted industries, the Company's ability to expand its sales and professional services organizations, the Company's ability to manage growth, the Company's ability to attract and retain qualified personnel, the Company's reliance on relationships with service vendors, the Company's reliance on licensed technology, the Company's ability to protect its proprietary rights, potential year 2000 problems, the Company's ability to compete in the rapidly evolving electronic compliance management market, the development and growth of the electronic compliance management market, the Company's ability to respond to changes in the electronic compliance management market, and other risks detailed in its Securities and Exchange Commission filings, including the Registration Statement on Form S-1.

CoreDossier is a registered trademark of ESPS, Inc.

PR Newswire Dec 21, 1999

ESPS Introduces Document Management System (DMS) Object Toolkit; Enables Integration Between ESPS' CoreDossier(R) Software and Custom DMS Products or Commercial DMS Products Not Yet Supported by ESPS.

FORT WASHINGTON, Pa., Dec. 21 /PRNewswire/ -- ESPS, Inc. (Nasdaq: ESPS), the premier provider of software and expertise that accelerate the assembly and publishing of business-critical knowledge, today introduced its Document Management System (DMS) Object Toolkit to help customers with their integration requirements between the ESPS CoreDossier(R) software and custom DMS products or commercial DMS products that ESPS does not currently support. The DMS Object Toolkit is available for CoreDossier, versions 4.0 and greater.

"Using this Toolkit, ESPS has built integrations for CoreDossier and commercial DMS products from DOCUMENTUM, FileNET, PC DOCS, Lotus Notes and Open Text*," said Mike Hoey, vice president of research & development at ESPS. "CoreDossier presently can create publications built from source documents stored in these DMS products, as well as shared file systems. The new DMS Toolkit will enable expansion of the use of CoreDossier to those companies using niche or industry-specific DMS products. Some of these DMS vendors have a strong presence in new markets for ESPS and availability of the Toolkit will expedite ESPS' entrance into these areas."

One ESPS partner, Provenance, the leading provider of Electronic Recordkeeping Systems (ERS), is already using a beta version of the DMS Toolkit to build an integration to its ERS software product, ForeMost. "The DMS Toolkit has allowed us to easily and quickly complete integration features," said Russ Stalters, vice president of professional services and customer support at Provenance. "The use of a standard interface has eliminated the learning curve, saving us tremendous time in the integration process."

CoreDossier helps companies accelerate the assembly and publishing of mission-critical knowledge for paper and electronic consumption -

- regardless of where the knowledge is stored in the organization. The integration between CoreDossier and a DMS allows a company to leverage its investment in both products by using each product to its full capacity. CoreDossier meets a DMS at the point where a business requirement drives the need to create a publication that contains multiple documents of multiple formats from the DMS.

"The new DMS Object Toolkit, along with the existing CoreDossier API set, allows systems integrators to expand the publishing capabilities of CoreDossier to new business environments," said Jeff Klein, director of document management services at First Consulting Group. "The integration of CoreDossier input and output with a DMS can be a powerful tool for organizations that manage the creation, assembly, and consumption of complex documents."

While the majority of DMS users are often information creators, CoreDossier users are primarily information assemblers, taking different components and marrying them together as one conceptually logical unit, and reviewers, consuming the final publication with user-friendly navigation tools and paradigms.
The DMS Object Toolkit provides everything that a third party needs to integrate CoreDossier with their Document Management System. A CoreDossier/DMS integration can range from a simple integration, allowing only intra/inter-publishing of DMS documents to an all-encompassing set of features, including:

-- Adding DMS source documents into CoreDossier publications

-- Importing DMS compound document structures into CoreDossier

publications

-- Exporting CoreDossier(R) publication structures into DMS compound

document structures

-- Transformation of over 80 source formats into PDF with automatic check-

in of document PDFs as renditions into the DMS

-- Automatically checking in CoreDossier-generated TOCs to the DMS

-- Automatically checking in published output as PDF source files into the

DMS

-- Navigating published output from within the DMS client

-- Displaying of DMS client dialogs for document property information

-- Batch checking in of file system documents into the DMS

-- Publishing of DMS compound documents to CoreDossier directly from

within the DMS client

-- Processing of DMS rendition queue jobs

Since the ESPS DMS object is two ActiveX Controls packaged as a standard Microsoft COM DLL, developers with a working knowledge of client/server applications and Microsoft COM/ActiveX can build an integration using the defined specifications in the Toolkit. The Toolkit also provides instructions, required header files and sample files for the ESPS DMS object.

For those requiring assistance building an integration, ESPS can provide expert consulting services. With in-depth experience developing custom applications, ESPS consultants can help create applications to match customers' unique requirements.

*OpenText is currently under development

About ESPS

ESPS, Inc. provides software and expertise that accelerate the planning, assembling, managing, publishing, and sharing of business-critical knowledge for paper, portals and the Web. ESPS is the leading developer of solutions that address the needs of companies faced with regulatory compliance submission requirements through the application of industry expertise, advanced technology and a commitment to high-quality implementations. The ESPS CoreDossier(R) software suite has set the standard for electronic compliance management in industries, including pharmaceutical, chemical and utilities. The ESPS world headquarters is located in suburban Philadelphia, with additional offices throughout North America and in Europe. More information can be found at www.esps.com, or by reaching the Company at 800-515-ESPS (North America) or +44 (0) 1753 725203 (Europe).

The statements in this news release which are not historical facts are forward-looking statements. These forward-looking statements involve risks and uncertainties that could render them materially different, including, but not limited to, the effect of fluctuations in the Company's operating results, the Company's reliance on a limited number of significant customers, the Company's reliance on

the CoreDossier product family, the Company's ability to market and sell its products and services in its targeted industries, the Company's ability to expand its sales and professional services organizations, the Company's ability to manage growth, the Company's ability to attract and retain qualified personnel, the Company's reliance on relationships with service vendors, the Company's reliance on licensed technology, the Company's ability to protect its proprietary rights, potential year 2000 problems, the Company's ability to compete in the rapidly evolving electronic compliance management market, the development and growth of the electronic compliance management market, the Company's ability to respond to changes in the electronic compliance management market, and other risks detailed in its Securities and Exchange Commission filings, including the Registration Statement on Form S-1.

CoreDossier is a registered trademark of ESPS, Inc.

PR Newswire April 13, 2000

ESPS Signs Global Corporate License Agreement with Merck KGaA.

Merck KGaA to Use Both CoreDossier(R) & kPublisher(TM) Software

FORT WASHINGTON, Pa., and DARMSTADT, Germany, April 13 /PRNewswire/ --

ESPS, Inc. (Nasdaq: ESPS), the premier provider of knowledge publishing solutions for the eWorld, today announced that the Company signed Merck KGaA as a new global customer for its knowledge publishing software, making this one of the largest license agreements ever for ESPS. With the new software, Merck plans to enhance its global publishing environment in the research and development area.

CoreDossier(R) and the new kPublisher(TM) software are part of the ESPS Knowledge Publishing Suite(TM), a complete, one-stop solution for publishing corporate knowledge, enabling companies to more effectively plan, manage, assemble, share and publish both electronic and paper publications. CoreDossier enables compound document assembly and publishing for large, complex publications. kPublisher offers Web-enabled knowledge assembly and publishing focused on small- to mid-range reports and documents. The output generated from CoreDossier and kPublisher can quickly and effectively be consumed by the business user community either electronically or on paper. Faster and more effective business decisions, improved time-to-market for new products, and achieving regulatory compliance are a few examples of key benefit gains.

"Our agreement with Merck, a success for the ESPS European team, further expands the traditional ESPS pharmaceutical market, illustrating global interest in this space for CoreDossier and our new kPublisher," said Rick Dool, executive vice president of sales and marketing at ESPS. "Utilizing both products in tandem within their publishing environment offers valuable sharing of intellectual property throughout Merck's research and development group."

Knowledge publishing is the creation of complex information components, using multiple input sources (over 130 file formats supported) with diverse output options. Input sources can be many file formats, including text, spreadsheets, presentations, drawings, graphs, mpeg, avi, real-time audio and video. Outputs include Web portals, e-mail, CD-ROM, document repositories and paper.

"We at Merck plan to roll out ESPS' publishing software first within the research and development area in Germany, with expansion to France, the U.S. and beyond," said Michael Baroth, project manager at Merck KGaA. "Both software tools are key to supporting our efforts to streamline the publishing processes in R&D."

About ESPS

ESPS, Inc. provides knowledge publishing solutions that accelerate the assembly, management and exchange of diverse business-critical information for the eWorld. Since 1995, ESPS has been the leading developer of ePublishing software products that address the needs of companies faced with compound document publishing requirements through the application of industry expertise, advanced technology and a commitment to high-quality implementations. The ESPS world headquarters is located in suburban Philadelphia, with additional offices throughout North America and in Europe. More information can be found at http://www.esps.com, or by reaching the Company at 800-515-ESPS (North America), or 1753-725203 (Europe).

The statements in this news release which are not historical facts are forward-looking statements. These forward-looking statements involve risks and uncertainties that could render them materially different, including, but not limited to, the effect of fluctuations in the Company's operating results, the Company's reliance on a limited number of significant customers, the Company's reliance on the knowledge publishing product family, the Company's ability to market and sell its products and services in its targeted industries, the Company's ability to expand its sales and professional services organizations, the Company's ability to manage growth, the Company's ability to attract and retain qualified personnel, the Company's reliance on relationships with service vendors, the Company's reliance on licensed technology, the Company's ability to protect its proprietary rights, the Company's ability to compete in the rapidly evolving electronic compliance management market, the development and growth of the electronic compliance management market, the Company's ability to respond to changes in the electronic compliance management market, and other risks detailed in its Securities and Exchange Commission filings, including the Registration Statement on Form S-1.

The ESPS Knowledge Publishing Suite is a trademark of ESPS, Inc.
